(12) UK Patent Application (19) GB (11) 2 332 973 (13) A

(43) Date of A Publication 07.07.1999

(21) Application No 9828569.5

(22) Date of Filing 23.12.1998

(30) Priority Data
(31) 09000624 (32) 30.12.1997 (33) US

(51) INT CL[6]
A61B 5/117

(52) UK CL (Edition Q)
G4R REX R1X
G4H HTG H1A H13D H14A
U1S S1719 S1725 S1727 S1729 S1741 S1792 S1819 S1839 S2123 S2312 S2322

(56) Documents Cited
GB 2270588 A WO 94/22371 A2 WO 87/02491 A1
US 5594806 A US 5055658 A US 4993068 A

(58) Field of Search
UK CL (Edition Q) G4H HTG, G4R REP RET REX RPF RPQ RRH RRL RRM RRQ
INT CL[6] A61B 5/00 5/117, G06K 9/00, G07C 9/00
Online:WPI

(71) Applicant(s)
Accu-Time Systems Inc
(Incorporated in USA - Connecticut)
420 Somers Road, Ellington, Connecticut 06029, United States of America

(72) Inventor(s)
Peter C DiMaria

(74) Agent and/or Address for Service
Stevens Hewlett & Perkins
1 Serjeant's Inn, Fleet Street, LONDON, EC4Y 1NT, United Kingdom

(54) Abstract Title
Biometric interface device

(57) An existing personal control system upgraded by replacing each of the personnel data input units of an existing personal control unit 40 with a biometric interface terminal 10 capable of reading physical characteristics. The personnel control unit 40 controls access based upon a signal from its terminal 10. Each terminal is also connected to an existing host 50 which is programmed to permit access, entry and/or egress for certain personnel, based upon authorisation information. The host 50 is connected to a database 60 for storing the authorisation information and to a keyboard 70 and a display 80.

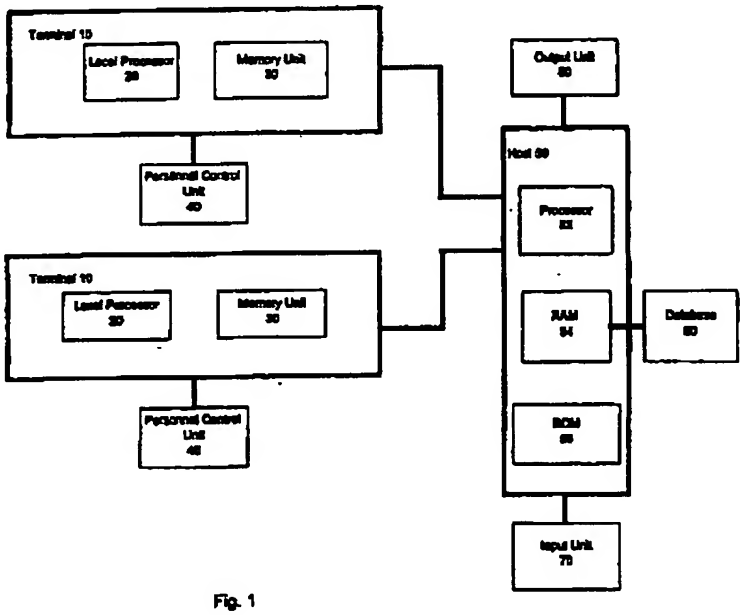

Fig. 1

GB 2 332 973 A

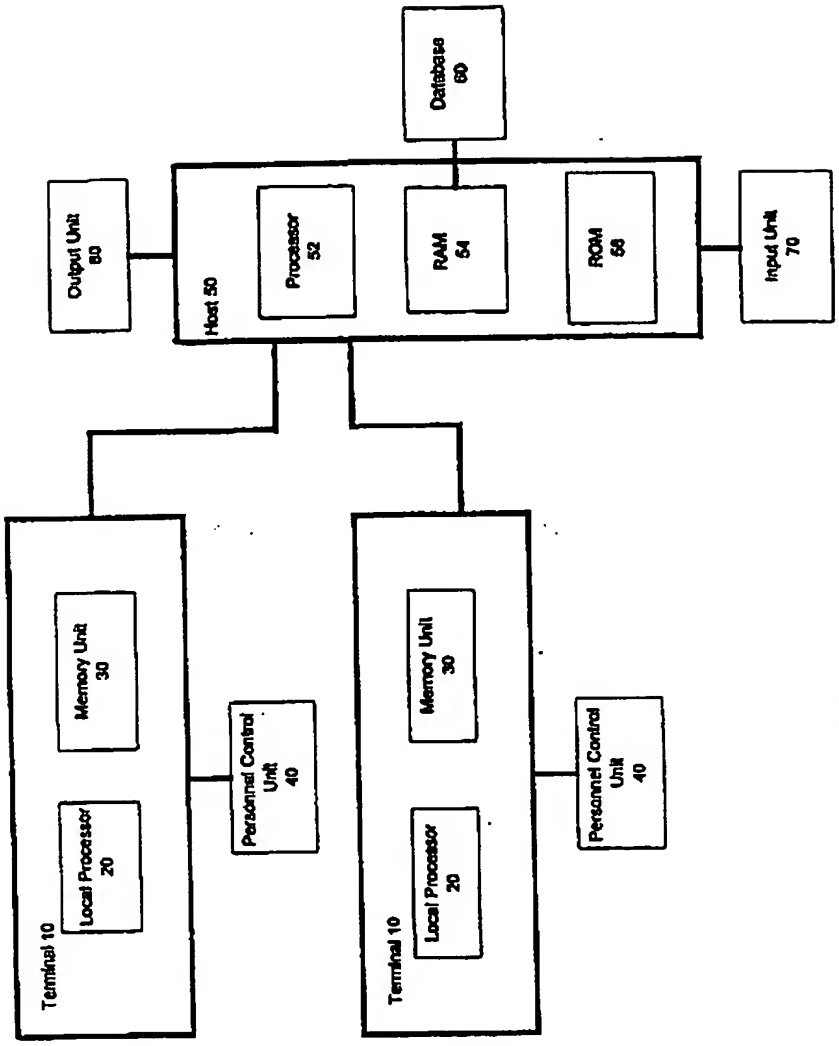
Database
60
Output Unit
80
Host 50
Processor
52
RAM
54
ROM
56
Input Unit
70
Terminal 10
Memory Unit
30
Local Processor
20
Personnel Control
Unit
40
Terminal 10
Memory Unit
30
Local Processor
20
Personnel Control
Unit
40

Fig. 1

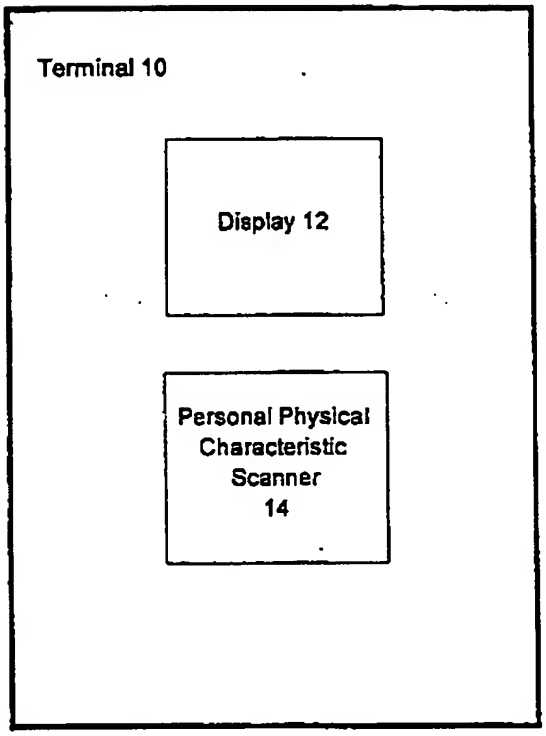
Terminal 10
Display 12
Personal Physical Characteristic Scanner 14

Fig. 2

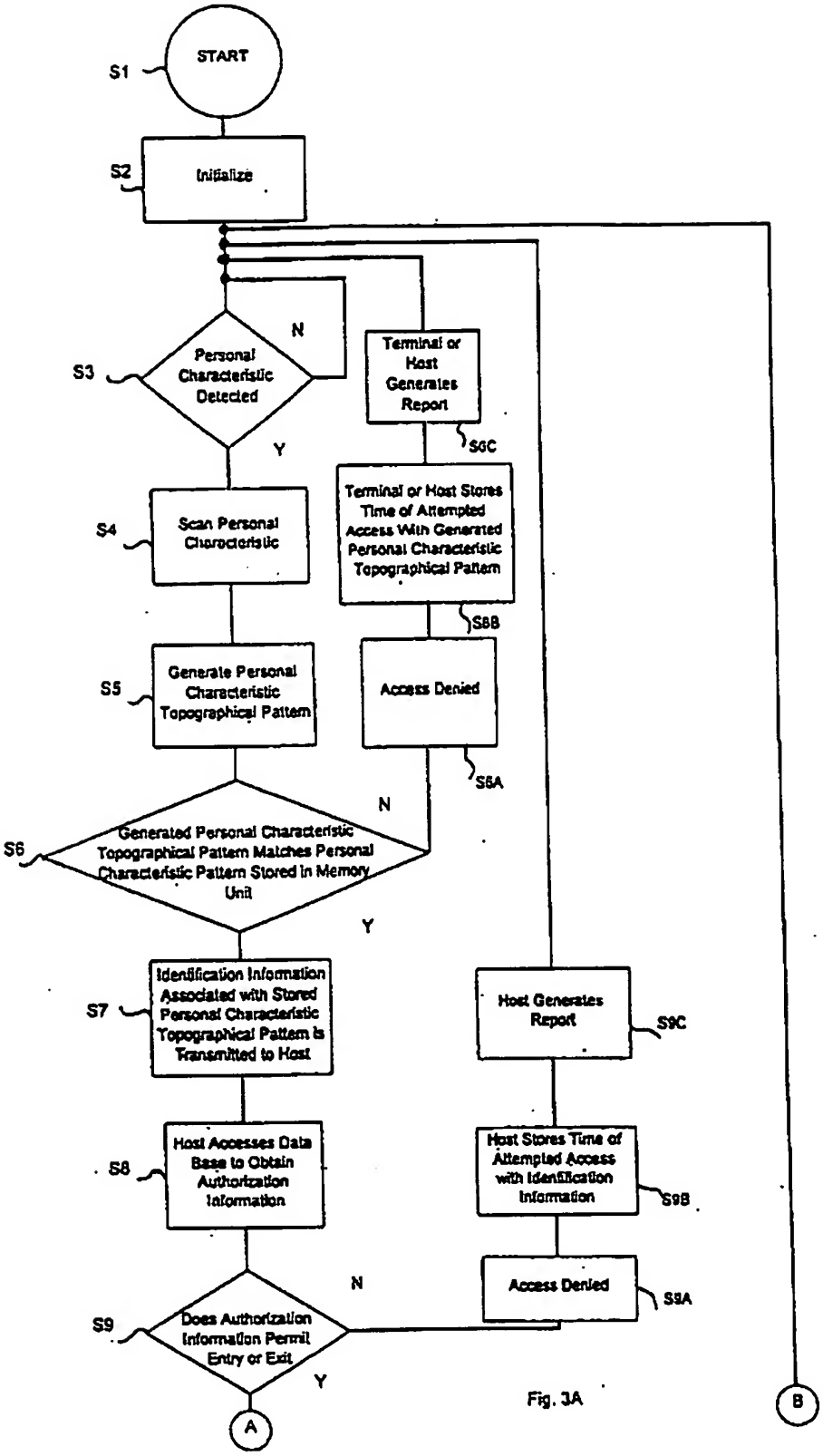
START
S1
Initialize
S2
Personal Characteristic Detected
S3
N
Y
Terminal or Host Generates Report
S8C
Terminal or Host Stores Time of Attempted Access With Generated Personal Characteristic Topographical Pattern
S8B
Scan Personal Characteristic
S4
Generate Personal Characteristic Topographical Pattern
S5
Access Denied
S8A
Generated Personal Characteristic Topographical Pattern Matches Personal Characteristic Pattern Stored in Memory Unit
S6
N
Y
Identification Information Associated with Stored Personal Characteristic Topographical Pattern is Transmitted to Host
S7
Host Generates Report
S9C
Host Accesses Data Base to Obtain Authorization Information
S8
Host Stores Time of Attempted Access with Identification Information
S9B
Access Denied
S9A
Does Authorization Information Permit Entry or Exit
S9
N
Y
A
B

Fig. 3A

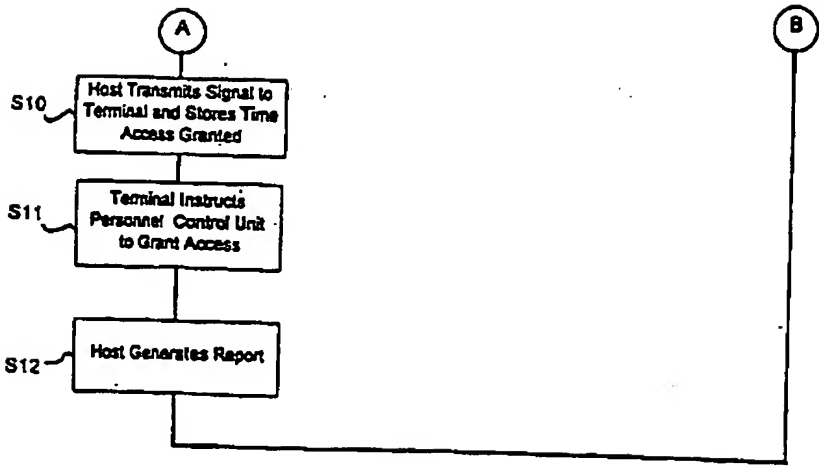
A
B
S10
Host Transmits Signal to Terminal and Stores Time Access Granted
S11
Terminal Instructs Personnel Control Unit to Grant Access
S12
Host Generates Report

Fig. 3B

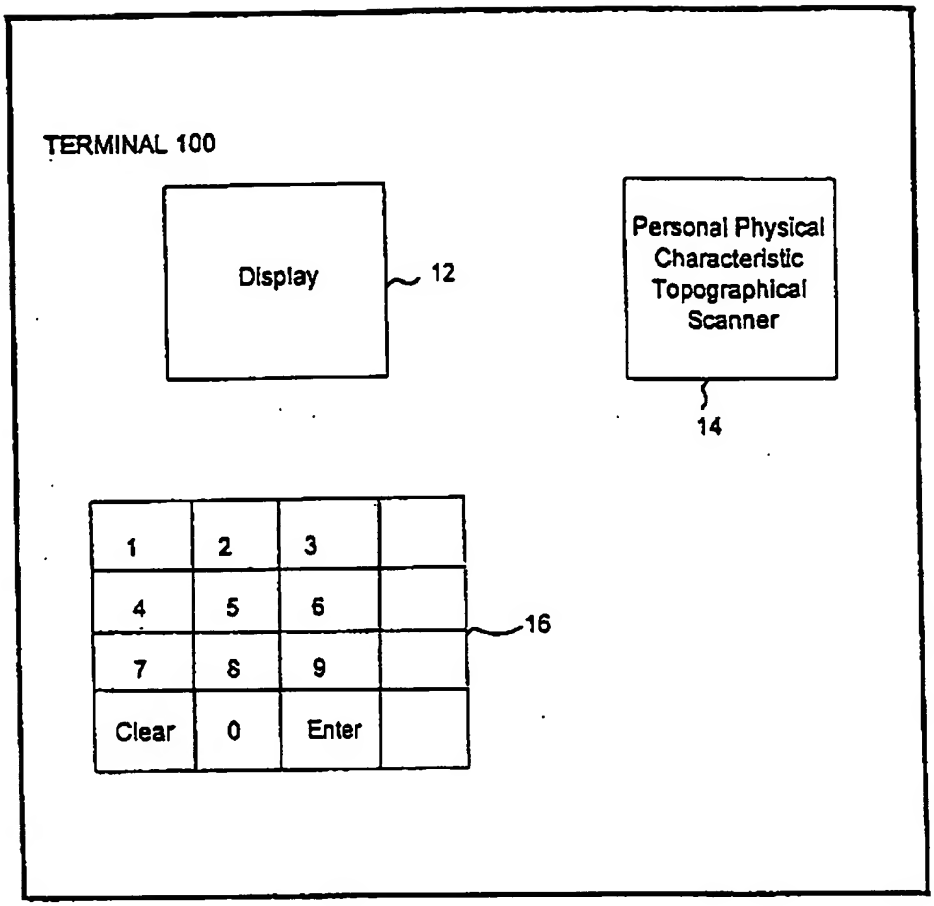
TERMINAL 100
Display
12
Personal Physical Characteristic Topographical Scanner
14
1
2
3
4
5
6
7
8
9
Clear
0
Enter
16

Fig. 4

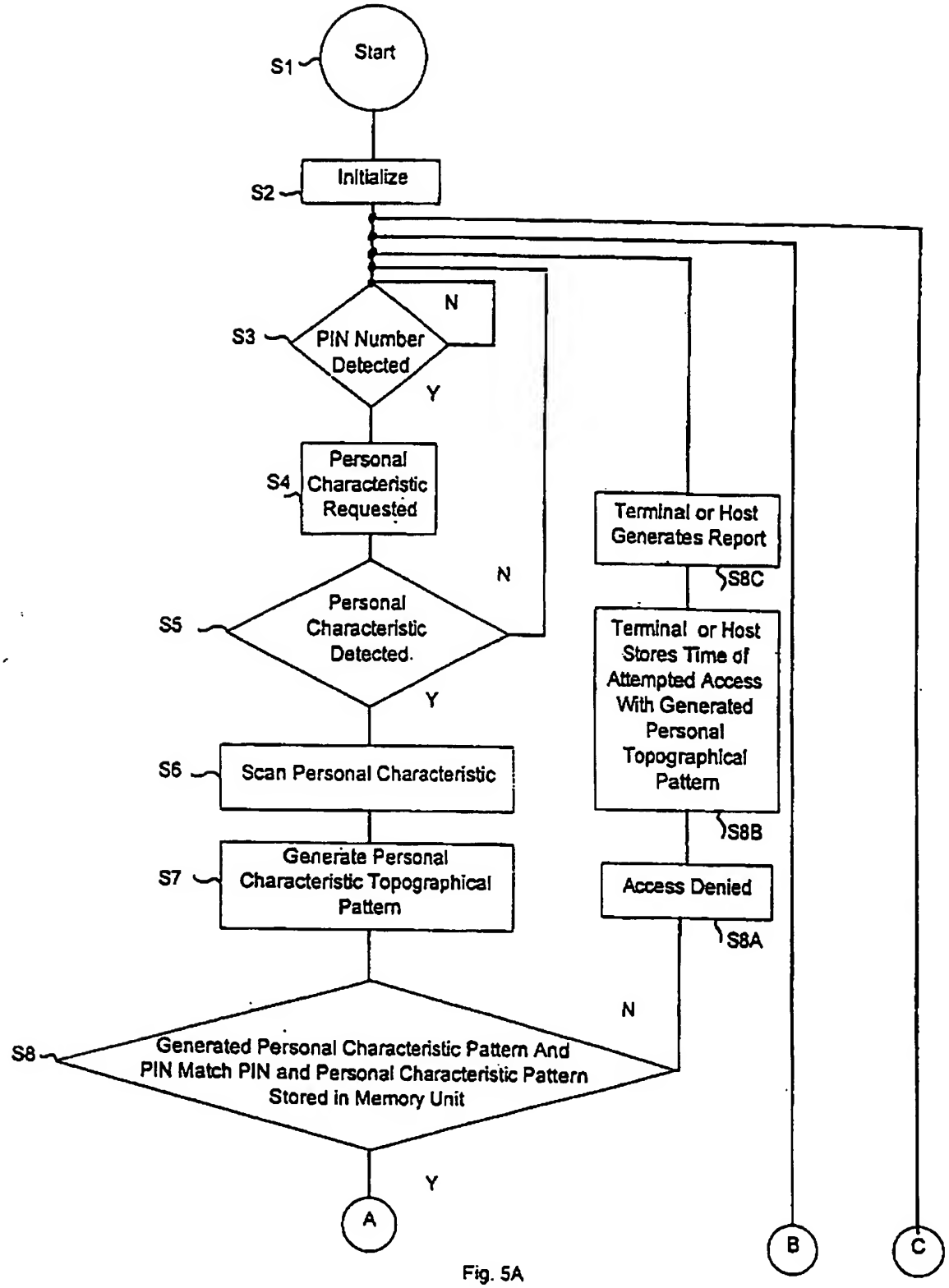
Start
S1
Initialize
S2
PIN Number Detected
S3
N
Y
Personal Characteristic Requested
S4
Personal Characteristic Detected.
S5
N
Y
Scan Personal Characteristic
S6
Generate Personal Characteristic Topographical Pattern
S7
Generated Personal Characteristic Pattern And PIN Match PIN and Personal Characteristic Pattern Stored in Memory Unit
S8
N
Y
A
Terminal or Host Generates Report
S8C
Terminal or Host Stores Time of Attempted Access With Generated Personal Topographical Pattern
S8B
Access Denied
S8A
B
C

Fig. 5A

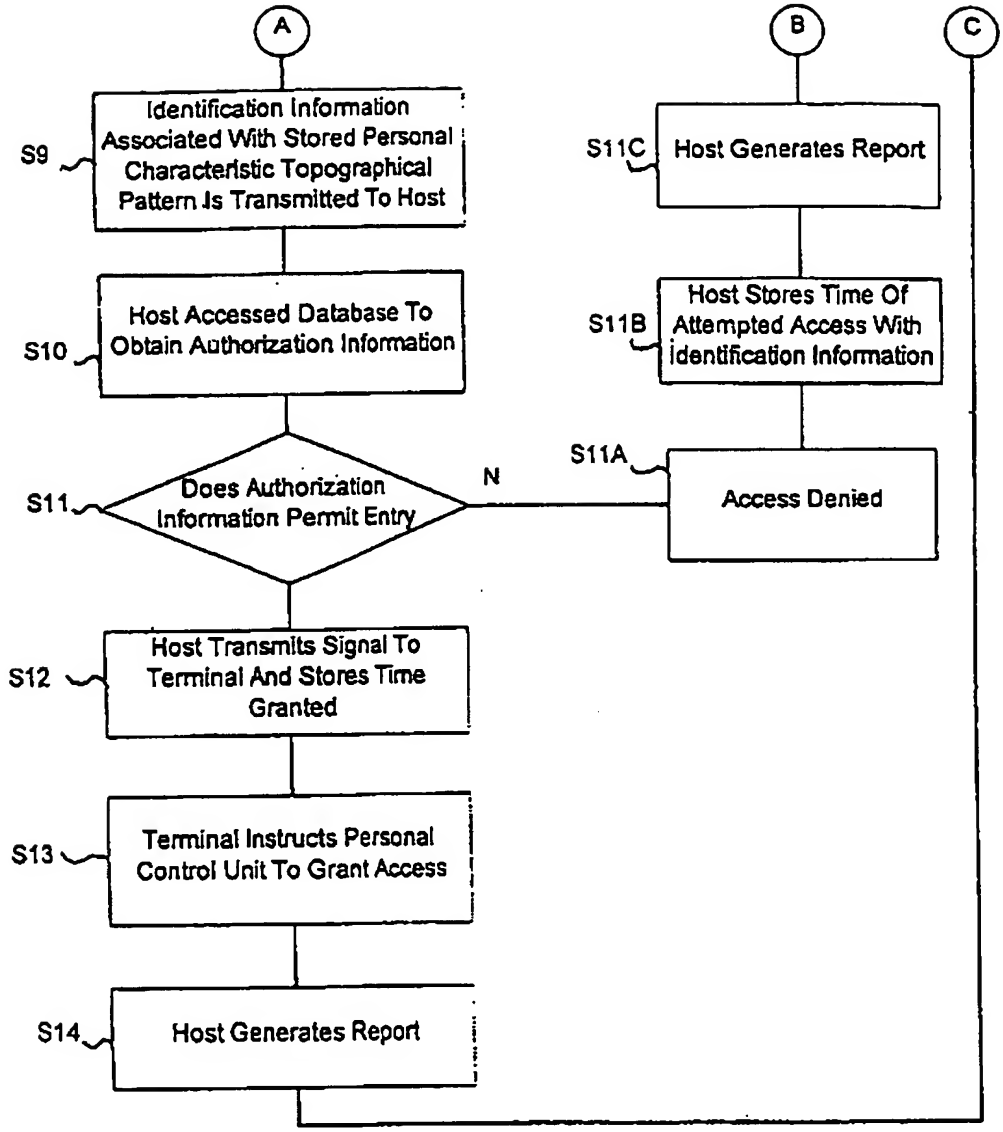
A
B
C
S9
Identification Information Associated With Stored Personal Characteristic Topographical Pattern Is Transmitted To Host
S10
Host Accessed Database To Obtain Authorization Information
S11
Does Authorization Information Permit Entry
N
S11A
Access Denied
S11B
Host Stores Time Of Attempted Access With Identification Information
S11C
Host Generates Report
S12
Host Transmits Signal To Terminal And Stores Time Granted
S13
Terminal Instructs Personal Control Unit To Grant Access
S14
Host Generates Report

Fig. 5B

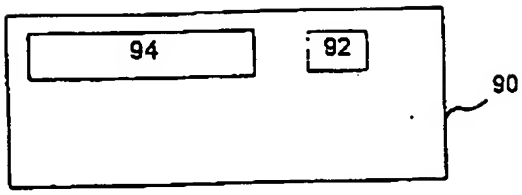

Fig. 6

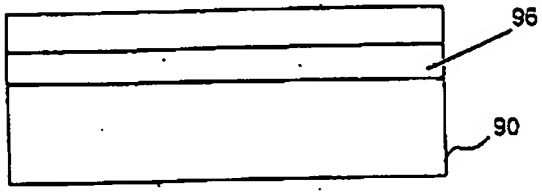

Fig. 7

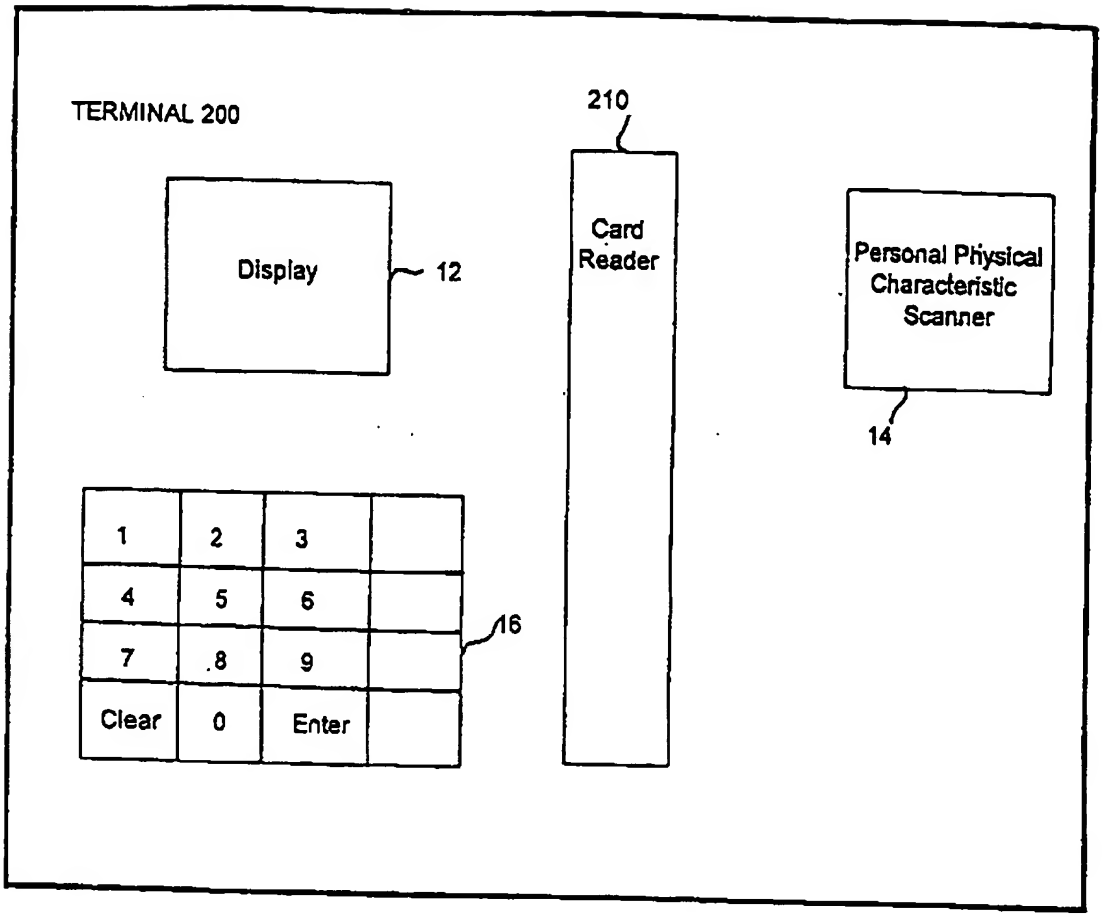
TERMINAL 200
210
Card Reader
Display
12
Personal Physical Characteristic Scanner
14
1
2
3
4
5
6
7
8
9
Clear
0
Enter
16

Fig. 8

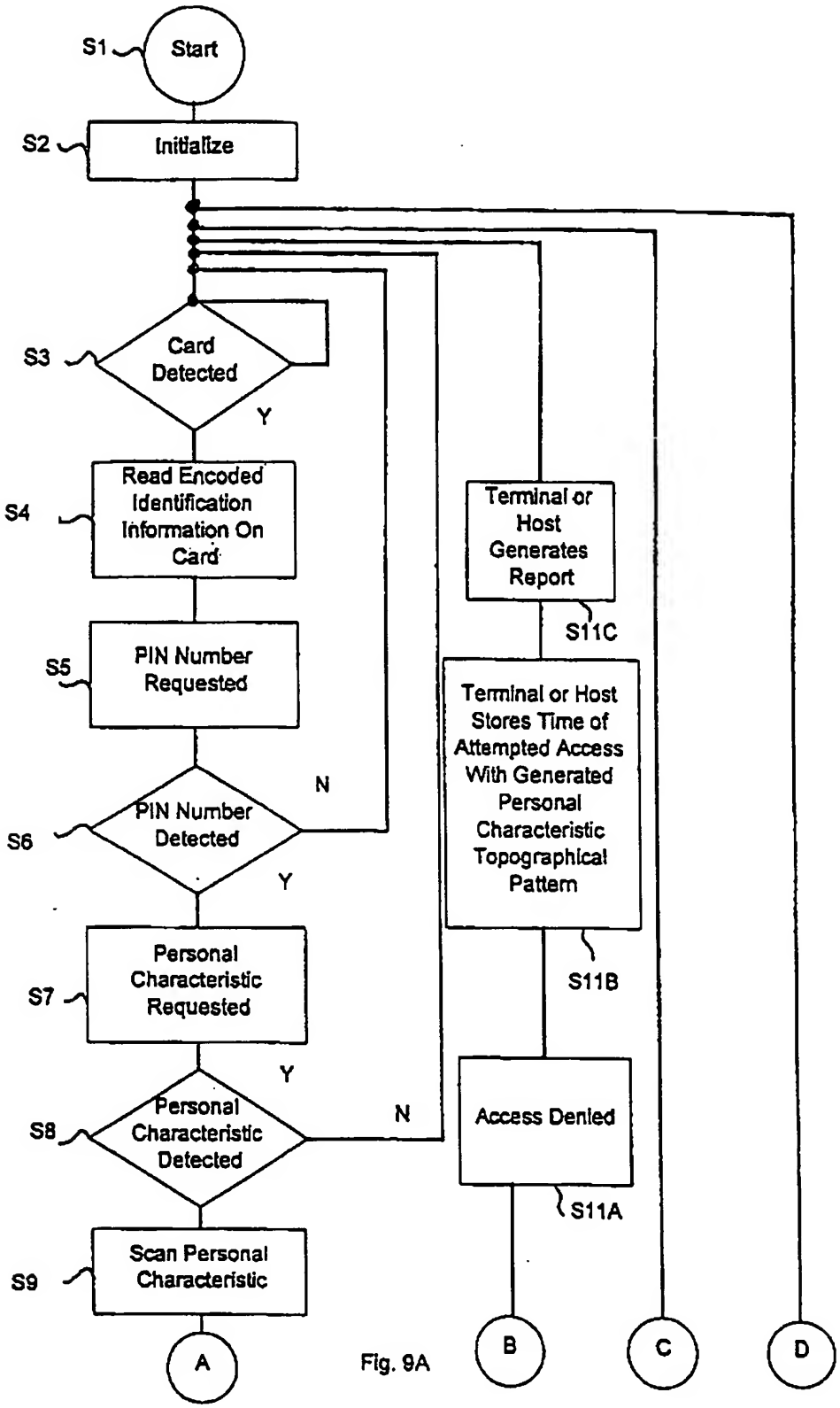
S1
Start
S2
Initialize
S3
Card Detected
Y
S4
Read Encoded Identification Information On Card
S5
PIN Number Requested
S6
PIN Number Detected
N
Y
S7
Personal Characteristic Requested
Y
S8
Personal Characteristic Detected
N
S9
Scan Personal Characteristic
A
Terminal or Host Generates Report
S11C
Terminal or Host Stores Time of Attempted Access With Generated Personal Characteristic Topographical Pattern
S11B
Access Denied
S11A
B
C
D

Fig. 9A

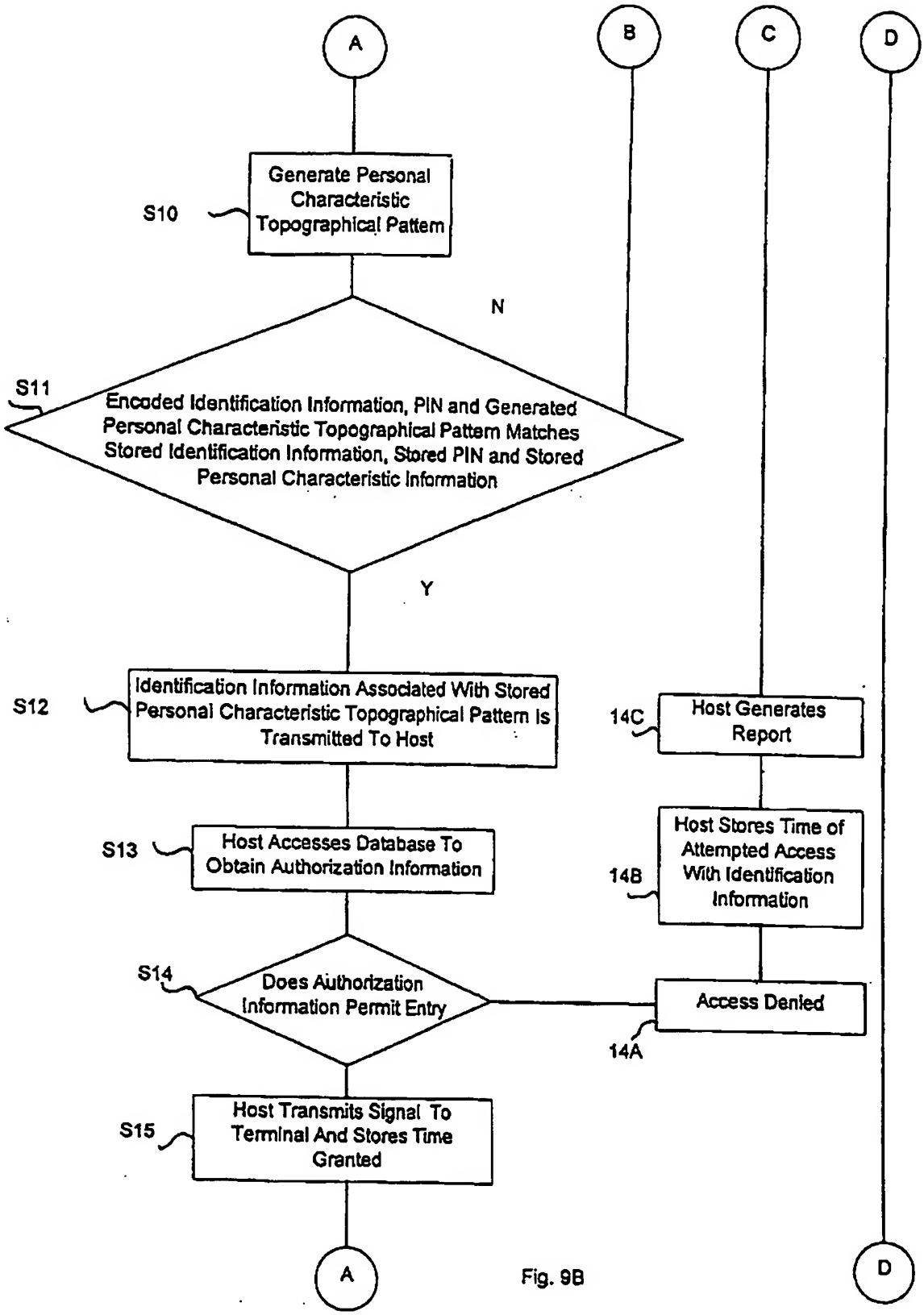
A
B
C
D
Generate Personal Characteristic Topographical Pattern
S10
N
S11
Encoded Identification Information, PIN and Generated Personal Characteristic Topographical Pattern Matches Stored Identification Information, Stored PIN and Stored Personal Characteristic Information
Y
S12
Identification Information Associated With Stored Personal Characteristic Topographical Pattern Is Transmitted To Host
14C
Host Generates Report
S13
Host Accesses Database To Obtain Authorization Information
14B
Host Stores Time of Attempted Access With Identification Information
S14
Does Authorization Information Permit Entry
Access Denied
14A
S15
Host Transmits Signal To Terminal And Stores Time Granted
A
D

Fig. 9B

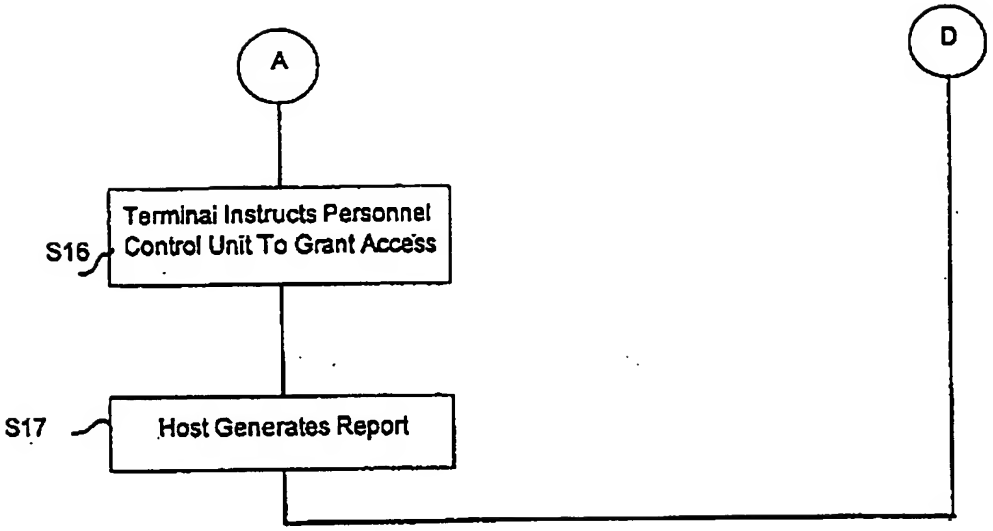
A
D
Terminal Instructs Personnel Control Unit To Grant Access
S16
S17
Host Generates Report

Fig. 9C

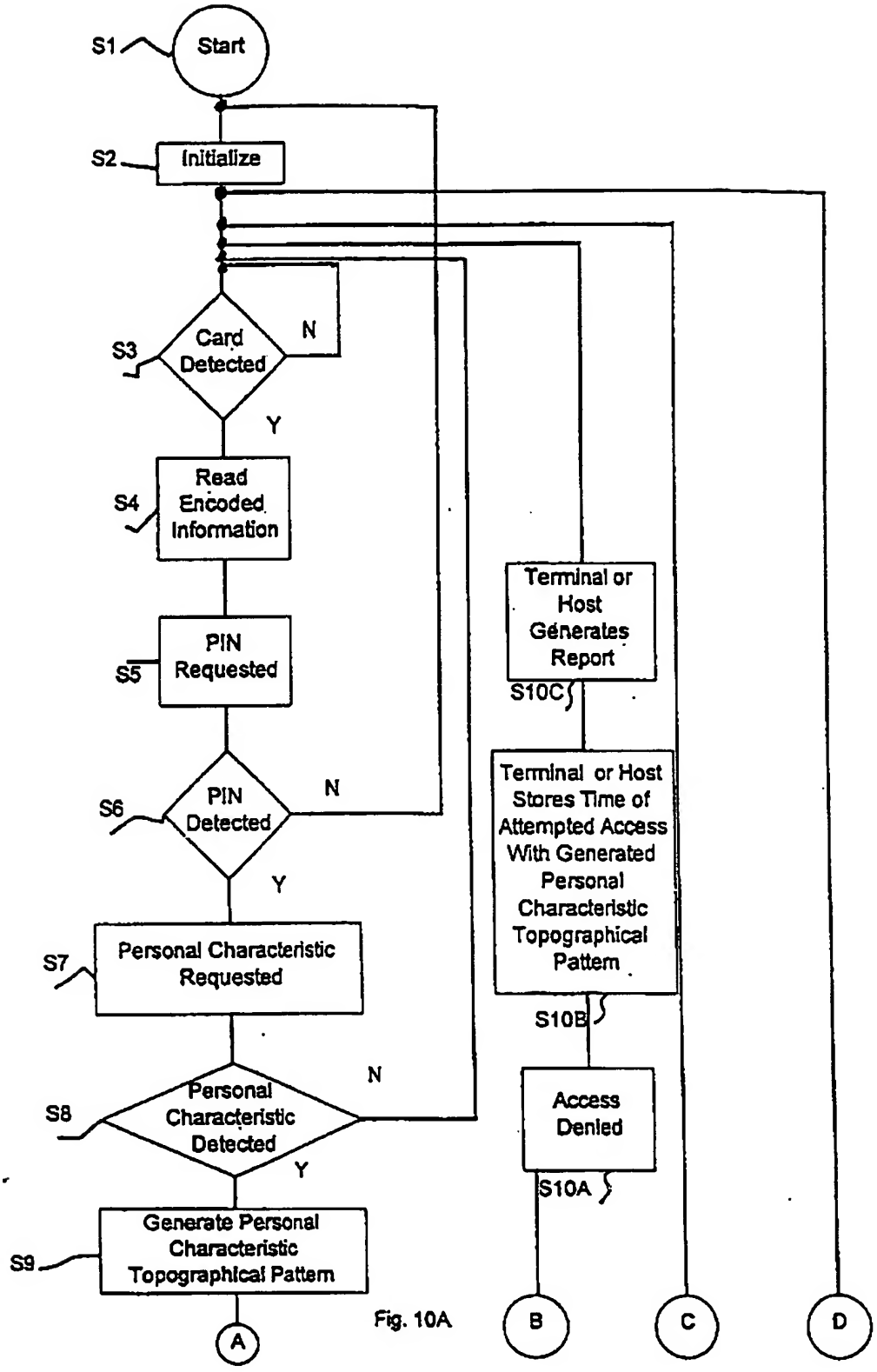
S1
Start
S2
Initialize
S3
Card Detected
N
Y
S4
Read Encoded Information
S5
PIN Requested
S6
PIN Detected
N
Y
S7
Personal Characteristic Requested
S8
Personal Characteristic Detected
N
Y
S9
Generate Personal Characteristic Topographical Pattern
A
Terminal or Host Generates Report
S10C
Terminal or Host Stores Time of Attempted Access With Generated Personal Characteristic Topographical Pattern
S10B
Access Denied
S10A
B
C
D

Fig. 10A

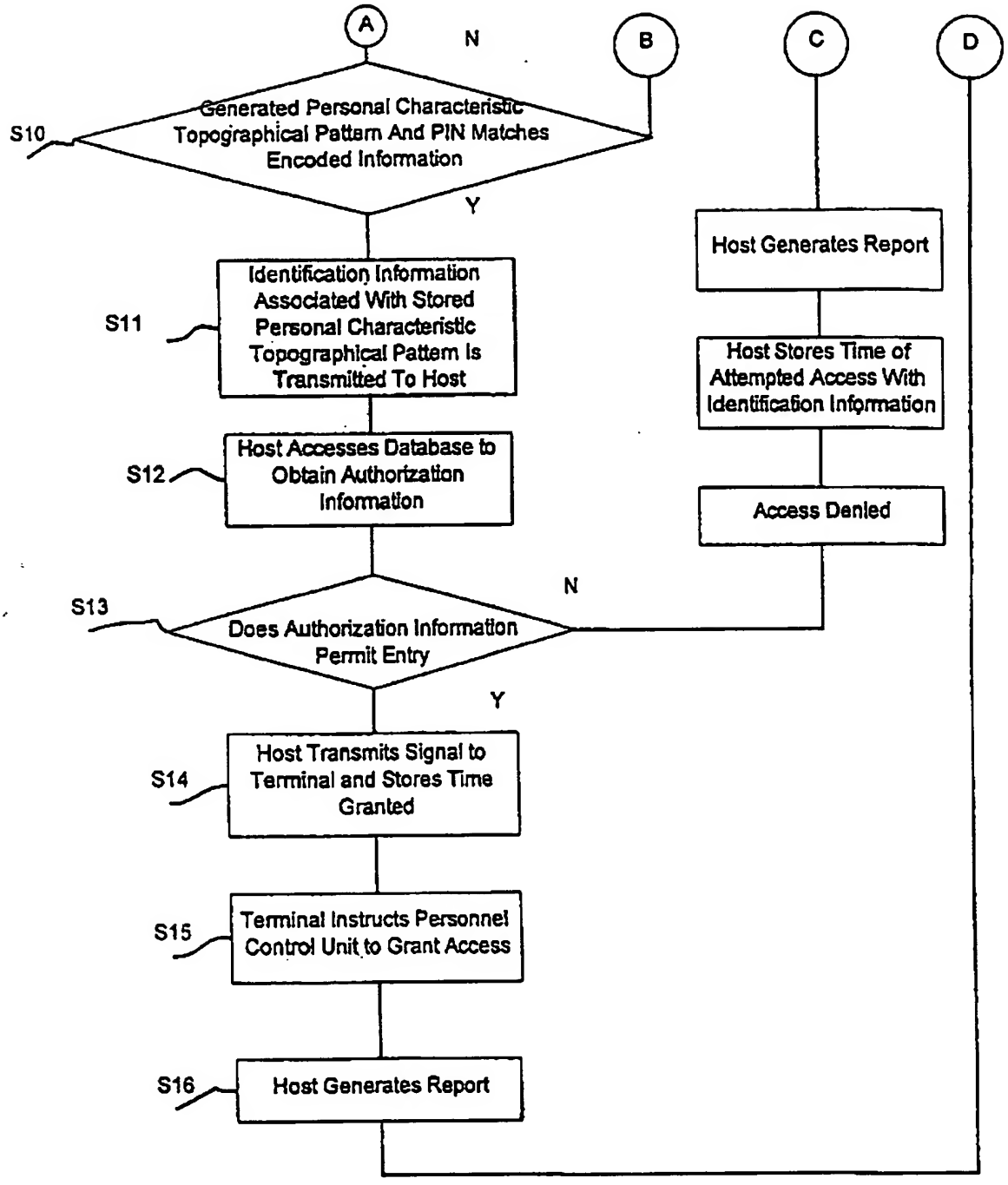
A
N
B
C
D
S10
Generated Personal Characteristic Topographical Pattern And PIN Matches Encoded Information
Y
Host Generates Report
S11
Identification Information Associated With Stored Personal Characteristic Topographical Pattern Is Transmitted To Host
Host Stores Time of Attempted Access With Identification Information
S12
Host Accesses Database to Obtain Authorization Information
Access Denied
N
S13
Does Authorization Information Permit Entry
Y
S14
Host Transmits Signal to Terminal and Stores Time Granted
S15
Terminal Instructs Personnel Control Unit to Grant Access
S16
Host Generates Report

Fig. 10B

BIOMETRIC INTERFACE DEVICE FOR UPGRADING EXISTING PERSONNEL CONTROL SYSTEMS

The present invention relates to a method and apparatus for upgrading existing personnel control systems. More particularly, the present invention relates to replacing the interface units of existing personnel control units with a biometric interface capable of outputting a signal compatible with the format of the currently installed personnel control system.

Increasingly, security problems are becoming a more noticeable part of modern life. Security was once primarily the preserve of classified government installations, but increasing losses and calamity have forced the review of security equipment and procedures for government and industry. Cargo losses and the theft of corporate secrets cost industry billions of dollars annually. Public safety is endangered by the ability of intruders to access secured places, such as aircraft and airport buildings.

Personnel control and personal identification are daily problems, and continue to be the object of significant expenditures by organizations needing to identify employees, vendors, etc., who are to be allowed access to the secured areas. Typical personnel control applications include:

computer center; radioactive or biological danger areas; controlled experiments; information storage areas; airport maintenance and freight areas; hospital closed areas and drug storage areas; apartment houses and office buildings; manufacturing facilities and construction sites; safety deposit boxes and vaults; and computer terminal entry and access to information.

Obtaining an individual's identity is a common problem in any access control application. Many existing personnel control applications establish a person's identity using a personal identification code or a card having encoded identification information. More recently, in order to increase security, some organizations are installing biometric devices with personnel control capabilities. These devices electronically scan a personal physical characteristic of an individual, such as a portion of the epidermis or human eye. After scanning a personal physical characteristic, these devices generate a pattern which is compared against a library of patterns that identifies the individuals permitted access to a controlled area.

For example, U.S. Patent No. 3,581,282 discloses a palm print identification system. In one example, a number code, encoded on an I.D. card, uniquely identifies a palm of an individual. The system reads the I.D. card and the actual palm of the individual. The number code is used as an index to retrieve a stored palm print pattern. Then, the stored palm print pattern is compared to the fresh palm print pattern to verify the identity of the individual.

U.S. Patent No. 4,210,899 discloses a fingerprint-based personnel control and identification apparatus. The apparatus reads a human fingerprint and transmits an electronic representation of the fingerprint to a centralized image processing unit. The centralized image processing unit determines access to certain areas, terminals or doors based on the specific fingerprint read.

U.S. Patent No. 5,337,043 discloses a personnel control system using data stored in the form of a barcode. A fingerprint pattern of the keyholder is stored in the form of a barcode on the key. After the key is placed on the keyway of a terminal at a personnel control point and read, the keyholder may then be prompted to place a finger against the fingerprint reader. The fingerprint is scanned and compared at the access control point terminal with the key encoded information. If a match is made, the personnel control point decision and the keyholder identifying code are sent to a remote central processor or host computer. The central processor determines whether a keyholder is permitted to access a particular area at the particular time that the card is read. A signal indicating that access is granted or denied is sent to the terminal.

U.S. Patent No. 5,195,145 provides an apparatus which scans a fingerprint and provides positive confirmation of an individual's identity at a particular location at a particular time. The terminal utilizes fingerprint scanners with magnetic cardreaders to reduce fraud in credit card

transactions by sending the scanned card and fingerprint to a credit verification company.

All these new biometric devices are not compatible with the presently installed personnel control devices which establish a person's identity utilizing a personal identification code or encoded card. Often, presently installed devices must be deactivated or removed, which adds to the expense of installing a new control access system. Therefore, there is a need for an inexpensive biometric interface device to upgrade existing personnel control units.

The present invention provides a biometric interface device for interfacing with an existing personnel control system of a type that utilize individualized stored data for the purpose of determining access authorization.

In one embodiment, the biometric interface device associates a library of personal physical characteristic topographical patterns, such as epidermal topographical patterns, with identification information stored in a memory. When a topographical pattern is read by the biometric interface device, it is compared against the entries of associated identification information stored in a memory unit. If there is a match, the identification information may be transmitted to a host computer in the format of the currently installed system. The host computer may use the identification information as an index to ascertain whether the individual is authorized to access a controlled area. For

added security, the subject individual may also be required to input a personal code and present an identification document containing machine readable data to be scanned or read. If access is authorized, the host transmits an authorization signal in the format of the currently installed system.

Alternatively, the personal characteristic topographical pattern is stored on an identification document in a machine readable code. The terminal reads the document, scans the personal characteristic and performs a comparison. If there is a match, the identification information may be transmitted to a host computer in the format of the currently installed system. The host computer accesses the data base to obtain authorization information. If the individual is authorized, the host transmits an authorization signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of an embodiment of the present invention;

Figure 2 is a block diagram of a front face of a first embodiment of a terminal of the present invention;

Figures 3A and **3B** are diagrams of the steps of controlling access utilizing the terminal of the first embodiment of the present invention;

Figure 4 is a block diagram of a front face of a second embodiment of a terminal of the present invention;

Figures 5A and 5B are diagrams of the steps of controlling access utilizing the terminal of the second embodiment of the present invention;

Figure 6 is a block diagram of a typical card;

Figure 7 is a block diagram of the rear face of the typical card;

Figure 8 is a block diagram of a front face of a third embodiment of a terminal of the present invention;

Figures 9A through 9C are diagrams of the steps of controlling access utilizing the terminal of the third embodiment of the present invention; and

Figures 10A and 10B are diagrams of alternative steps of controlling access utilizing the terminal of the third embodiment of the present invention.

The preferred embodiments are described with reference to drawing figures wherein like numerals represent like elements throughout.

Figure 1 shows a plurality of terminals 10 having a local processor 20 and memory unit 30. Each terminal 10 is substituted for an existing terminal and is preferably connected to an existing personnel control unit 40. The personnel control unit 40 controls access based upon a signal from the terminal 10. Each terminal 10 is also preferably connected to an existing host 50 which includes a processor 52, RAM 54 and a ROM 56. The host 50 is preferably programmed to permit access, entry and/or egress, for certain personnel

based upon authorization information. Authorization information preferably includes a list of personnel controlled areas and times during which an individual is to be permitted access. For example, an individual may be permitted access only during a specified work shift. The authorization information would include the permitted area(s) and the permitted time(s) for that individual. Since the authorization information is under the employer's control, the permitted access area(s) and time(s) can be changed easily without the need for the issuance of a new individual identification card or a manual check of updated access information by security personnel. The host 50 has a database 60 for storing the authorization information and is connected to an input unit 70, such as a keyboard, and an output unit 80, such as a liquid crystal display.

Figure 2 is a diagram of a first embodiment of the terminal of the present invention. The terminal 10 includes a display 12 and a personal characteristic scanner 14 as well as the local processor 20 and memory unit 30. Examples of the personal characteristic scanner 14 include an epidermal topographical scanner and an eye scanner. Examples of epidermal topographical scanners include fingerprint scanners, knuckleprint scanners, handprint scanners and palmprint scanners. Examples of eye scanners include iris scanners and retina scanners. The personal characteristic scanner reads an individual's personal characteristic and generates a personal characteristic pattern which is compared to stored personal characteristic patterns.

The operational flow of a first embodiment of the terminal 10 is shown in Figure 3. After the terminal 10 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). When a personal characteristic is detected (S3), the personal characteristic scanner 14 scans the personal characteristic (S4) and a personal characteristic topographical pattern is generated (S5). The local processor 20 compares the generated pattern to a library of patterns stored in memory unit 30 (S6). If there is no match, access is denied (S6A). The terminal 10 may transmit the time of attempted access and the generated personal characteristic topographical pattern to the host 50 for storage in the database 60 (S6B). Alternatively, the terminal 10 may store the time of attempted access and the generated personal characteristic topographical pattern in the memory unit 30. The host 50 or terminal 10 may generate a report of the attempted access(S6C). Thereafter, the system returns to step S3.

If there is a match, identification information associated with the stored personal characteristic topographical pattern is transmitted to the host 50 (S7). The host 50 accesses the database 60 to obtain authorization information regarding the individual seeking access (S8). If the authorization information associated with the identification information in the database 60 permits access (S9), the host 50 transmits a signal to the terminal 10 and stores the access time (S10). The terminal 10 instructs the personal control unit 40 to grant access (S11) and the host

50 generates a report (S12), and the system returns to step S3.

If the authorization information does not permit access (S9A), the host 50 stores the time of attempted access with the generated physical characteristic topographical pattern in the data base 60 (S9B). The host 50 may also generate a report of the attempted access (S9C). Thereafter, the system returns to step S3.

It will be recognized that a principal advantage of the present invention is the ability to replace an existing access control device, such as a barcode scanner, with a personal characteristic identification control apparatus without the need for modifying the existing system. Since the present invention provides an output that is compatible with the existing system, the change will appear seamless to the current host. The ability to avoid the need for changes in software or hardware provides an economic advantage that greatly enhances the added feature of a physical characteristic identification system.

Figure 4 is a diagram of a second embodiment of a terminal of the present invention. The terminal 100 preferably includes the same apparatus as terminal 10. In addition to the local processor 20, memory unit 30, display 12 and personal physical characteristic topographical scanner 14, the terminal 100 also includes a keypad 16 for receiving a personalized code, such as a PIN, which is required to gain access.

The operational flow of a second embodiment of the present invention utilizing terminal 100, is shown in Figures 5A-5B. After the terminal 100 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). When a personal code is detected (S3), the terminal 100 requests a personal characteristic (S4). When a personal characteristic is detected (S5), the personal characteristic is scanned (S6) by the scanner 14 and a personal characteristic pattern is generated (S7). The local processor 20 compares the newly generated personal characteristic pattern and personal code with the library of corresponding data stored in memory unit 30 (S8).

If there is no match, access is denied (S8A), and the host 50 or terminal 100 stores the time of attempted access with the generated physical characteristic topographical pattern in the data base 60 or memory unit 30 (S8B). The host 50 or terminal 100 may also generate a report of the attempted access (S8C). Preferably, the terminal 100 stores the information and generates the report. Thereafter, the system returns to step S3.

If there is a match, the identification information associated with the stored personal characteristic topographical pattern is transmitted to the host 50 in a format compatible with the existing system (S9). The host 50 accesses database 60 to obtain authorization information regarding the individual seeking access (S10). If the authorization information does not permit entry or exit, access is denied (S11A) and the host 50 stores the time of

attempted access with the identification information (S11B). Subsequently, the host 50 generates a report (S11C) and the system returns to step S3.

If there is a match, the host 50 transmits a signal to the terminal 100 in the existing format and stores the time access is granted. The terminal 100 instructs the personal control unit 40 in the existing format to grant access (S13) and the host 50 generates a report (S14). Thereafter, the system returns to step S3.

Figures 6 and 7 show an example of an identification document 90, which is read by a terminal 200 (Figure 8) in a third embodiment of the present invention. In order to gain access, an individual is required to present an identification document 90 having at least one machine readable medium. Figure 6 shows the front face of an identification document 90 having a photograph 92 and a visible machine readable code 94. The identification document 90 may also contain personal identification information such as the bearer's name, eye color, personal characteristic information, etc. The same personal identification information may be encoded in a visible machine readable code 94. Figure 5 shows the rear face of the identification document 90 which includes a magnetic stripe 96. Personal identification information from a front face of the identification document 90 and personal characteristic information are preferably encoded on the magnetic stripe 96.

Referring to Figure 8, a block diagram of a third embodiment of the present invention is shown. The terminal

200 is substituted for the terminal 10 in Figure 1. In addition to the local processor 20, memory unit 30, display 12, and personal topographical scanner 14, the terminal 200 further includes a keypad 16 for receiving a personal code, such as a PIN, and a card reader 210 for reading either visible machine readable code 94 or encoded data on a magnetic stripe 96. The reader 210 may be configured to read both 94 and 96. The personal characteristic topographical scanner 14 reads a personal characteristic and generates a personal characteristic pattern.

Operation of the third embodiment of the present invention is shown in the flowchart in Figure 9. After the terminal 200 is activated, the program is started (S1) and the system is initialized, preferably automatically (S2). Once the identification document 90 is detected (S3), the identification document 90 is read to obtain encoded identification information (S4). A personal code is requested (S5). If a code is not entered, the system returns to step S3. If a code is detected, the system requests a personal characteristic (S7). If a personal characteristic is not detected by scanner 14, the system returns to step S3. If a personal characteristic is detected, it is scanned (S9) by scanner 14 and a personal characteristic pattern (S10) is generated.

If the encoded identification information, personal code, and generated personal characteristic pattern does not match the identification information, code, and personal characteristic information retrieved from memory unit 30,

access is denied. The host 50 or terminal 200 stores the newly presented encoded identification information, code and generated personal characteristic information in database 60 or memory unit 30. The host 50 or terminal 200 generates a report (S11A-S11C), and the system returns to S3.

If the encoded identification information, code and generated personal characteristic pattern matches stored identification information, code and personal characteristic pattern retrieved from the memory unit 30, an identification information signal is transmitted to the host 50 (S12).

Once the host 50 receives the identification information signal, the host 50 accesses the database 60 to obtain authorization information (S13). If the authorization information does not permit entry, access is denied (S14A) and the host 50 stores time of attempted access with the identification information (S14B). The host 50 generates a report (S14C) and returns to step S3. If the authorization information permits entry, the host 50 transmits a signal in the existing format to the terminal 200 and stores the time access is granted. The terminal 200 instructs the personal control unit 40 in the existing format to grant access (S16). The host 50 generates a report (S17), and the system returns to step S3.

Alternatively, the same terminal 200 may be programmed to provide a fourth embodiment of the present invention. Operation of the fourth embodiment of the present invention is shown in Figure 10. After the terminal 200 is activated, the program is started (S1) and the system is initialized,

preferably automatically (S2). After the card is detected, the machine readable code is read or scanned to obtain the encoded personal characteristic information (S4). A personal code is requested (S5). If a code is detected, a personal characteristic is requested (S7). If the personal characteristic is detected (S8), a personal characteristic pattern is generated by scanner 14 (S10).

If there is no match, access is denied (S11A), and the host 50 or terminal 200 stores the time of attempted access with the generated physical characteristic topographical pattern in the data base 60 (S11B). The host 50 or terminal 200 may also generate a report of the attempted access (S11C). Thereafter, the system returns to step S3.

If the generated personal characteristic pattern matches the encoded information and personal identification number (S11), the identification information associated with the stored personal characteristic topographical pattern is transmitted to the host 50 (S8). The host 50 accesses the database 60 to obtain authorization information (S12). If the authorization information permits entry then the host 50 transmits a signal in the existing format to a terminal 200 and stores the time access is granted (S13-S14). The terminal 200 instructs the personnel control unit 40 to grant access (S15) in the existing format and the host 50 generates a report (S16). If authorization is not permitted, access is denied, the host 50 stores the time of attempted access and the host 50 generates a report (13A-13C). The system then returns to step S3.

* * *

CLAIMS

1. An apparatus for interfacing with an existing personnel control system of a type that utilizes stored data, including personal topographical characteristic patterns, for the purpose of determining an individual's access authorization in a controlled area, the apparatus comprising:

means for scanning a predetermined physical characteristic of a presented individual;

means for generating a signal containing a topographical characteristic pattern of the scanned physical characteristic;

means for accessing the stored data;

means for comparing the generated pattern with the stored patterns, determining the individual's access authorization, and producing an authorization signal; and

means for communicating the authorization signal to the existing control system in a format that is compatible therewith.

2. The apparatus of claim 1, wherein the stored data is in a host data base.

3. The apparatus of claim 1, wherein the comparing means is a host computer.

4. The apparatus of claim 1, wherein the personal physical characteristic scanner is a fingerprint scanner and the stored topographical patterns are fingerprint patterns.

5. The apparatus of claim 1, wherein the personal physical characteristic scanner is a palm print scanner and the stored topographical patterns are palm print patterns.

6. The apparatus of claim 1, wherein the personal physical characteristic scanner is a knuckle print scanner and the stored topographical patterns are knuckle print patterns.

7. The apparatus of claim 1, wherein the personal physical characteristic scanner is an epidermal topographical scanner and the stored topographical patterns are epidermal topographical patterns.

8. The apparatus of claim 1, wherein the personal physical characteristic scanner is an eye scanner and the stored topographical patterns are stored eye patterns.

9. An apparatus of claim 1, wherein the personal physical characteristic scanner is a retina scanner and the stored topographical patterns are retina patterns.

10. The apparatus of claim 1, wherein the personal physical characteristic scanner is an iris scanner and the stored topographical patterns are iris patterns.

11. A method for interfacing a personal physical characteristic recognition device with an existing personnel control system, comprising:

associating a personal physical characteristic pattern with corresponding identifying information stored in a data base;

providing a scanner for scanning a personal physical characteristic;

developing a personal physical characteristic pattern signal from the scanner results;

comparing the scanned pattern signal with the stored patterns in the data base;

reviewing the corresponding identification information in storage; and

providing an authorization signal based upon the pattern comparison and data reviewed in a format compatible with the existing personnel control system.

12. The method of claim 11, wherein the scanner is an epidermal scanner and the stored patterns in the database are epidermal topographical patterns.

13. The method of claim 11, wherein the scanner is an eye scanner and the stored patterns in the database are eye topographical patterns.

14. The method of claim 11, wherein the scanner is an iris scanner and the stored patterns in the database are iris topographical patterns.

15. The method of claim 11, wherein the scanner is a retina scanner and the stored patterns in the database are retina topographical patterns.

16. An apparatus for interfacing with an existing personnel control system, comprising:

an identification document reader reading an encoded personal physical characteristic topographical pattern stored on an identification document;

a personal physical characteristic scanner scanning a predetermined portion of an individual and generating a personal physical characteristic topographical pattern; and

means for comparing the generated personal physical characteristic topographical pattern with the stored personal physical characteristic topographical pattern, and producing an authorization signal recognizable by the existing personnel control system.

17. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access based upon the content of the existing personnel control signal.

18. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access to a controlled area.

19. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access to information.

20. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access to a vehicle.

21. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access to a computing device.

22. An apparatus as in claim 16 wherein the existing personnel control system permits or denies access to a communication device.

23. An apparatus as in claim 16 wherein the personal physical characteristic scanner is an epidermal scanner and the stored personal physical characteristic topographical patterns are epidermal topographical patterns.

24. An apparatus as in claim 16 wherein the personal physical characteristic scanner is a fingerprint scanner and the stored personal physical characteristic topographical patterns are fingerprint patterns.

25. An apparatus as in claim 16 wherein the personal physical characteristic scanner is a palm print scanner and the stored personal physical characteristic topographical patterns are palm print patterns.

26. An apparatus as in claim 16 wherein the personal physical characteristic scanner is a knuckle print scanner and

the stored personal physical characteristic topographical patterns are knuckle print patterns.

27. An apparatus as in claim 16 wherein the personal physical characteristic scanner is an eye scanner and the stored personal physical characteristic topographical patterns are stored eye patterns.

28. An apparatus as in claim 16 wherein the personal physical characteristic scanner is a retina scanner and the stored personal physical characteristic topographical patterns are retina patterns.

29. A method for interfacing a personal physical topographical recognition device within an existing access control system, comprising:

providing an identification document scanner;

scanning and decoding an encoded physical characteristic pattern stored on the identification document;

providing the personal physical characteristic topographical scanner;

scanning a personal physical characteristic then generating a personal physical characteristic topographical pattern;

comparing said read personal physical characteristic topographical pattern with said scanned personal physical characteristic topographical pattern; and

providing the identification verification signal recognizable by the existing access control system based upon said comparing step.

30. The method of claim 29, wherein the personal physical characteristic scanner is an epidermal scanner and the digital personal physical characteristic topographical patterns stored in the database are epidermal topographical patterns.

31. The method of claim 29, wherein the personal physical characteristic scanner is an eye scanner and the digital personal physical characteristic topographical patterns stored in the database are eye topographical patterns.

32. The method of claim 29, wherein the personal physical characteristic scanner is an iris scanner and the digital personal physical characteristic topographical patterns stored in the database are iris topographical patterns.

33. The method of claim 29, wherein the personal physical characteristic scanner is a retina scanner and the digital personal characteristic topographical patterns stored in the database are retinal topographical patterns.

Amendments to the claims have been filed as follows

1. An apparatus for interfacing with an existing personnel control system that utilizes stored data in a predetermined format for the purpose of determining whether a presented individual is authorized to have access to a controlled area, the apparatus comprising:

means for storing physical characteristic information for a plurality of individuals;

means for storing for each individual, an access signal associated with the existing personnel control system;

means for scanning a physical characteristic of a presented individual;

means for generating a scanned physical characteristic signal for the presented individual;

means for comparing the stored physical characteristics information to the scanned physical characteristic signal to determine if a match is found;

means for outputting an access signal when a match is found; and

means for communicating the outputted access signal to the existing control system in a format that is compatible with the predetermined format of the stored data so that the existing personnel control system will recognize the outputted access signal as a match for the presented individual stored data and authorize access to the controlled area.

2 The apparatus of claim 1 wherein the predetermined format of the existing personnel control system is compatible with information stored on a card.

3. The apparatus of claim 2 wherein the card has a magnetic stripe and the stored information is encoded thereon.

4. The apparatus of claim 2 wherein the stored information is encoded on the card in machine readable code.

5. The apparatus of claim 1 wherein the predetermined format of the existing personnel control system is compatible with a PIN.

6. The apparatus of claim 1 further comprising means for denying access when a match is not found.

7. The apparatus of claim 1 further comprising means for storing a time of attempted access and the scanned physical characteristic when a match is not found.

8. A biometric apparatus for interfacing with an existing personnel control system that utilizes stored data, in addition to biometric data, for the purpose of determining

whether a presented individual is authorized to have access to a controlled area, the apparatus comprising:

means for storing biometric information for a plurality of individuals;

means for obtaining biometric information on a presented individual;

means for storing for each individual, an access signal associated with the existing personnel control system;

means for generating an obtained biometric information signal for the presented individual;

means for comparing the stored biometric information to the obtained signal to determine if a match is found;

means for outputting an access signal when a match is found; and

means for communicating the outputted access signal to the existing control system in a format that is compatible with the stored data so that the existing personnel control system will recognize the outputted access signal as a match for the presented individual stored data and authorize access to the controlled area.

The Patent Office

Application No:	GB 9828569.5	**Examiner:**	John Donaldson
Claims searched:	1 to 33	**Date of search:**	25 January 1999

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4R(REP, RET, REX, RPF, RPQ, RRH, RRL, RRM, RRQ); G4H(HTG)

Int Cl (Ed.6): A61B 5/00, 5/117; G06K 9/00, G07C 9/00

Other: Online:WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	GB 2270586 A	(MYTEC), see abstract	1 to 33
X	WO 94/22371 A2	(DIGITAL BIOMETRICS), see column 5, line 5 to column 8, line 33	1 to 33
X	WO 87/02491 A1	(BLACKWELL), see abstract	1 to 33
X	US 5594806	(COLBERT), see abstract	1 to 33
X	US 5055658	(COCKBURN), see abstract	1 to 33
X	US 4993068	(PIOSENKA), see abstract	1 to 33

25

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.